(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number: **0 602 335 A3**

(12) EUROPEAN PATENT APPLICATION

(21) Application number: **93115876.0**

(51) Int. Cl.[6] **H04L 9/08**

(22) Date of filing: **01.10.93**

(30) Priority: **15.12.92 US 991054**

(43) Date of publication of application:
22.06.94 Bulletin 94/25

(84) Designated Contracting States:
AT CH DE DK FR GB IE IT LI NL SE

(88) Date of deferred publication of the search report:
25.01.95 Bulletin 95/04

(71) Applicant: **MOTOROLA, INC.**
1303 East Algonquin Road
Schaumburg, IL 60196 (US)

(72) Inventor: **Barney, George M.**
8426 E. Cholla
Scottsdale,
Arizona 85260 (US)
Inventor: **Hardy, Douglas A.**
2207 E. Gable Avenue
Mesa,
Arizona 85204 (US)
Inventor: **Balogh, Craig R.**
838 E. Harmony Avenue
Mesa,
Arizona 85204 (US)

(74) Representative: **Hudson, Peter David et al**
Motorola
European Intellectual Property
Midpoint
Alencon Link
Basingstoke,
Hampshire RG21 1PL (GB)

(54) Cryptographic key management apparatus and method.

(57) A method for establishing a secure communications link between first (103, 380) and second (109, 390) terminals includes a step of exchanging (210) a first message. The first message contains information describing encryption devices and communications modes available within the terminals and user authentication information. The method also includes a step of selecting (219, 221, 222, 224), in at least one terminal (103, 109), a common key generation and ciphering algorithm. The method further includes steps of exchanging (230) a second message for providing data to form traffic keys, exchanging (250) a third message for synchronizing secure communications and initiating (270) secure communication.

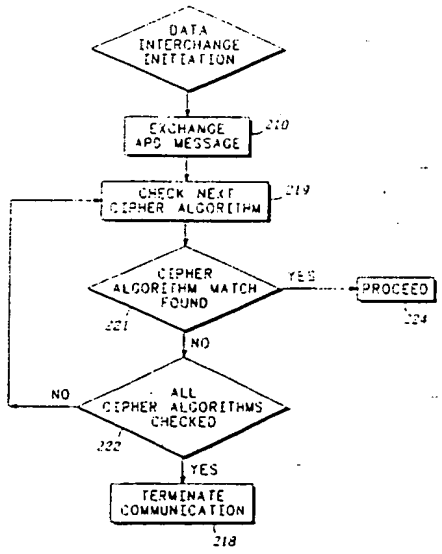

FIG. 4

EP 0 602 335 A3

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 93 11 5876

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.5)
P,X P,A	EP-A-0 537 971 (MOTOROLA) * the whole document * ---	1,4 3,5,6	H04L9/08 H04L9/00
Y	PROCEEDINGS OF THE INTERNATIONAL CARNAHAN CONFERENCE ON SECURITY TECHNOLOGY, 4 October 1983, ZURICH (CH) pages 95 - 102 CHORLEY ET AL. 'THE DEFINITION AND IMPLEMENTATION OF A SECURE COMMUNICATIONS PROTOCOL'	1	
A	* page 96, left column, line 23 - line 29 * * right column, paragraph 4 * * page 97, left column, line 6 - line 21 * * line 51 - page 98, right column, line 6 * * page 99, right column, last paragraph * ---	2,7	
Y	EP-A-0 364 866 (HAYES) * page 2, line 10 - line 16 * * page 7, line 58 - page 7, line 21 * * page 9, line 10 - line 14 * ---	1	
D,A	US-A-4 888 801 (FOSTER ET AL.) * column 2, line 50 - line 54 * * column 3, line 31 - line 46 * * column 4, line 23 - column 5, line 38 * ---	1,7	
A	1978 NATIONAL TELECOMMUNICATIONS CONFERENCE, vol.2, 3 December 1978, NEW YORK pages 26.1.1 - 26.1.6 LENNON 'CRYPTOGRAPHIC KEY DISTRIBUTION USING COMPOSITE KEYS' * page 26.1.2, left column, line 11 - line 34; figure 1 * * figure 3 * ---	3,5,6	
	-/--		

TECHNICAL FIELDS SEARCHED (Int.Cl.5)
H04L

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	28 November 1994	Holper, G

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 93 11 5876

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.5)
A	EP-A-0 162 962 (SIEMENS) * page 3, line 11 - line 15 * * page 4, line 24 - line 33 *	4	
A	US-A-4 763 357 (BARR) * column 1, line 58 - line 68 * * column 3, line 4 - line 7 * * line 37 - line 43 * * line 56 - line 63 * * column 5, line 66 - column 6, line 6 * * column 10, line 16 - line 37 *	1,7	
			TECHNICAL FIELDS SEARCHED (Int.Cl.5)

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	28 November 1994	Holper, G

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)